Reverse Engineering Report – Crackme Challenge

Author: Ali Rashchi

Date: 2025-08-09

Challenge: https://crackmes.one/crackme/682113c96297cca3ff7d7834

Title: Lilsan44444's Validator (easy)

Platform: Windows x86-64
Difficulty: 1.0
Language: C/C++

Objective

The objective of this challenge was to bypass both the debugger detection mechanism and the password validation check within the target executable, ultimately achieving the 'success' state without providing the correct base64-encoded password.

Tools Used

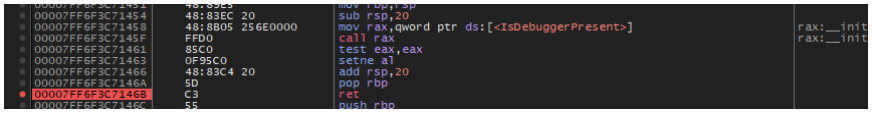
- x64dbg
- Windows 11 CMD

Methodology

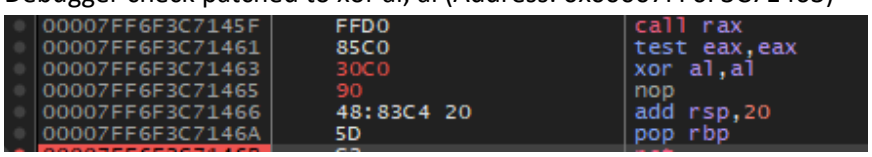
1. **Initial Analysis**: Loaded the crackme in x64dbg and located the anti-debugging function using the symbol `IsDebuggerPresent`.
2. **Debugger Bypass**: Patched the instruction `setne al` with `xor eax, eax` to force the zero flag state and avoid debugger detection.
3. **Password Check Bypass**: Identified the `test al, al` followed by a conditional jump (`je`) to the success message. Patched the conditional jump with NOP instructions to always execute the success branch.
4. **Final Test**: Executed the patched binary to verify that it bypasses both checks and displays the success message.

Screenshots and Addresses

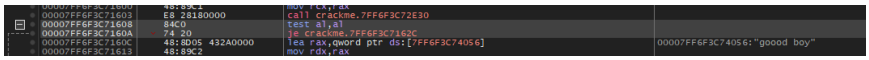
Screenshot showing debugger check function before patch (Address: 0x00007FF6F3C71463)



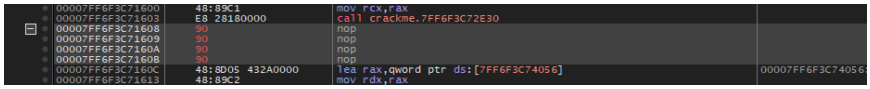
Debugger check patched to xor al, al (Address: 0x00007FF6F3C71463)



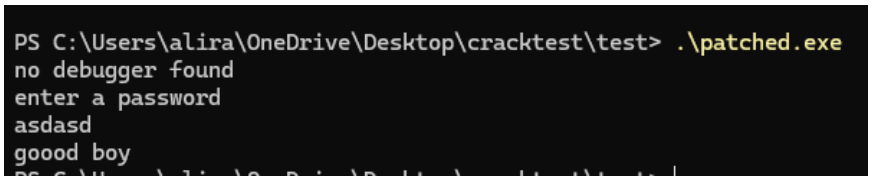
Password check before patch (Address: 0x00007FF6F3C7160A)



Password check patched with NOPs (Address: 0x00007FF6F3C7160A)



Patched executable output (Address: N/A)



Results

The patched executable successfully bypasses both the debugger presence check and the password validation routine, allowing access to the success message regardless of input. This demonstrates that both protections were effectively neutralized through binary patching.

Legal & Ethical Considerations

This work was performed exclusively for educational purposes on a publicly available crackme challenge designed for reverse engineering practice. The patched binary will not be redistributed. All modifications and analysis respect the platform's guidelines.

Contact: alirashchi7@gmail.com